CHANGE MANAGEMENT POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: February 10, 2021
Updated: February 10, 2021

NextGen CGI, LLC Change Management Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	02/10/2021	Policy	AF	CC	02/10/2021	SGH	02/10/2021

1. Overview

Operational change management brings discipline and quality control to Information Security. Attention to governance and formal policies and procedures will ensure its continued success. Adopting formalized governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalization requires communication, documentation of important process workflows and personnel roles, and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on the Information Security Senior Leadership Team to provide the guidance and vision to initiate the process. By defining processes and policies, organizations can demonstrate increased agility in responding predictably and reliably to new business demands.

2. Purpose

The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks, to include:

- Information being corrupted and/or destroyed
- Computer performance being disrupted and/or degraded
- Productivity losses being incurred
- Exposure to reputational risk

3. Scope

This policy applies to all parties operating within the company's network environment or utilizing information resources connection to the environment. It covers all data networks, servers, and personal computers located at company offices and affiliated locations. No employee or contractor is exempt from this policy.

4. Policy

Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner, and that the status of each proposed change is monitored.

4.1 Operational Procedures

4.1.1 The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (e.g. hardware, software, system documentation, and operating procedures). This documented process shall include management

responsibilities and procedures. Wherever practical, operational and application change control procedures should be integrated.

4.1.2 At a minimum, the change control process should include the following:

- Logged Change Requests
- Identification, Prioritization, and Initiation of change
- Documented authorization of change
- Requirements analysis
- Inter-dependency and compliance analysis
- Impact Assessment
- Change approach
- Change testing
- User acceptance testing and approval
- Implementation and release planning
- Change monitoring
- Defined responsibilities and authorities of all users and IT personnel
- Emergency change classification parameters

4.2 Documented Change

4.2.1 All change requests shall be logged, whether approved or rejected, in a standardized, central system. The approval and results of the change request shall be documented.

4.2.2 A documented audit trail, maintained at a Business Unit level, containing relevant information shall always be maintained. This should include change request documentation, change authorization, and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel.

4.3 Risk Management

4.3.1 A risk assessment shall be performed for all changes and dependent on the outcome, an impact assessment should be performed.

4.3.2 The impact assessment should include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable, consider compliance with legislative requirements and standards.

4.4 Change Classification

4.4.1 All change requests should be prioritized in terms of benefits, urgency, effort required and potential impact of operations.

4.5 Testing

4.5.1 Changes should be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

4.5.2 Reference the Software Development Lifecycle (SDLC) Policy for more information.

4.6 Changes Affecting SLAs

4.6.1 The impact of changes on existing SLAs should be considered. Where applicable, changes to the SLA should be controlled through a formal change process which includes contractual amendments as necessary.

4.7 Version Control

4.7.1 Any software change and/or update should be controlled with version control. Older versions should be retained in accordance with corporate retention and storage management policies.

4.8 Approval

4.8.1 All changes should be approved prior to implementation. Approval of changes should be based on formal acceptance criteria, such as ensuring that change requests were performed by an authorized user and impact assessments were performed and proposed changes were tested.

4.9 Communication Changes

4.9.1 All users that are or will be significantly affected by the change should be notified of the change. The user representative should sign-off on the change, and users should be required to make submissions and comments prior to acceptance of the change.

4.10 Implementation

4.10.1 Implementation will only be performed after appropriate testing and approval by stakeholders. All major changes should be treated as new system implementations and should be established as a project. Major changes will be classified according to effort required to develop and implement the change.

4.11 Fallback

4.11.1 Procedures for aborting and recovering from unsuccessful changes should be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities should be noted in the recovery and continuity of the affected areas.

4.11.2 Fallback procedures should always be in place and documented to ensure systems can revert to what they were prior to the implementation of the change.

4.12 Documentation

4.12.1 Information Resources documentation should be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

4.12.2 Information resources documentation is used for reference purposes in various scenarios (e.g. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable). It is therefore imperative that information

resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

4.13 Business Continuity Plan (BCP)

4.13.1 Business Continuity Plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy, and availability of BCP documentation. BCP documentation is the roadmap used to minimize disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

4.14 Emergency Changes

4.14.1 Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

4.15 Change Monitoring

4.15.1 All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

5. Roles and Responsibilities

Role	Functional Responsibilities
Members of the Board	• Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.
Information Security Manager	• Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries; • Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; • Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products; • Co-ordinate the overall communication and awareness strategy for change management; • Acts as the management champion for change management and control; • Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable.

	• Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and • Co-ordinate the implementation of new or additional security controls for change management.
Operations Manager	• Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; • Approve and authorize change management and control measures on behalf of the organization; • Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control; • Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums; • Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control; • Establish and revise the information security strategy, policy and standards for change management and control; • Facilitate and co-ordinate the necessary change management and control initiatives within each company; • Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control • Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/ version control solutions; and • Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company.

	• Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorizing, monitoring and enforcing change management initiatives and related security controls within all organizational companies and divisions; • Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control. Ensure the compliance of this policy and report deviations to the Information Manager.
IT Service Provider	• Shall comply with all change management and control statements of this policy.
Solution Owners	• Shall comply with all information security policies, standards and procedures for change management and control; and • Report all deviations.

6. Compliance

Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary or legal action in accordance with the NextGen CGI Disciplinary Code and Procedures. Company Information Security policies, standards, procedures and guidelines shall comply with legal, regulatory and statutory requirements.

7. IT Governance Value Statement

Changes that materially affect the financial process must be evaluated and reported quarterly. Financial system upgrades or replacements will require new certification. The implication is that Sarbanes-Oxley compliance is reliant on the changes you make to the operational systems and procedures.

8. Related Standards, Policies, and Processes

- Software Development Lifecycle (SDLC) Policy
- Business Continuity Plan
- Disaster Recovery Plan
- Physical and Environmental Protection Policy
- Data Protection Standard

9. Definitions and Terms

The following definition are not all-inclusive and should be updated as new information is made available:

Term	Definition
Audit Trail	A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such records.
Information Resources	All data, information, hardware, software, personnel and processes involved with the storage, processing and output of such information. This includes data networks, servers, PCs, storage media, printers, peripherals, and backup media.